REMARKS

Objections to the Drawings

In the Office Action, the Examiner objected to the drawings under 37 C.F.R. § 1.83(a). The Examiner requested that the Applicants provide a new drawing to further illustrate the claims. By the foregoing amendment, Applicants have provided new FIG. 5 which shows an exemplary system according to the present invention, in particular as is recited in claims 17-48. Additionally, Applicants have amended the "BRIEF DESCRIPTION OF THE DRAWINGS" section of the specification to describe new FIG. 5. No new matter has been added.

The Examiner also requested that a block diagram be provided to illustrate the method claims 1-13, 17-29, 33-45, 49 and 50. However, Applicants have amended the method claims such that they are more clearly illustrated by original FIGS. 3 and 4. Accordingly, Applicants respectfully request that the objections under 37 C.F.R. § 1.83(a) be withdrawn.

Claim Rejections under 35 U.S.C. § 112

In the Office Action, claims 1-13, 17-29, 33-45, 49 and 50 were rejected under 35 U.S.C. § 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains to make and use the invention. The Examiner expressed confusion regarding, in particular, the recitation in the claims of a "first transaction type" and a "second transaction type." Applicants have amended the claims to replace this language with language pertaining to an "ATM transaction" and "non-ATM transaction." Applicants respectfully submit that the above claims as amended are in compliance with § 112, first paragraph.

Additionally, claims 41-43 were rejected under § 112, second paragraph, as being indefinite. Claim 41 has been amended to remove informalities in accordance with the Examiner's remarks. Accordingly, Applicants submit that claims 41-43 as amended fully comply with § 112.

Claim rejections under 35 U.S.C. § 102(b)

In the Office Action, claims 1-5, 17-20, and 33-36 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Number 4,214,230 to Fak et al. (hereinafter "Fak"); claims 1, 6, 7, 12, 17, 22, 23, 28, 33, 38, 39, and 44 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Number 4,223,403 to Konheim et al. (hereinafter "Konheim"); and claims 14, 15 , 30, 31, 46, 47, 49 and 50 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Number 4,223,403 to Rosenow (hereinafter "Rosenow"). In view of Applicants' foregoing amendments and following remarks, reconsideration of the rejections of record is respectfully requested.

Regarding the rejection of claims 1-5, amended independent claim 1 recites a method for generating identification data, comprising the steps of, *inter alia*,

> providing an ATM PIN related to a first transaction type which is an ATM transaction; and
>
> performing a cryptographic operation upon the ATM PIN, thereby generating a non-ATM electronic commerce PIN for use in a second transaction which is a non-ATM transaction.

Fak describes a method and apparatus for verifying that the bearer of a card is authorized to use the card. (See Fak, Abstract). As described in the portion of Fak cited in the Office Action, an account number and PIN are assigned to a cardholder, and a check number (PCN) is derived by generating a first cipher by encrypting the check number using the PIN in combination with a secret security number as a key. (See Fak,

col. 2, lines 3-11). Fak fails to disclose several features recited in amended claim 1. First, Fak does not disclose performing a cryptographic operation on an ATM PIN to generate a non-ATM electronic commerce PIN for use in a non-ATM electronic commerce transaction (See, e.g., Specification, p. 4, wherein a user enters the non-ATM PIN in the course of a non-ATM electronic transaction). More generally, Fak does not disclose any type of cryptographic relationship between two different PIN numbers. Accordingly, because Fak fails to disclose at least these limitations of independent claim 1 as amended, Applicants respectfully request that this rejection be withdrawn. Additionally, dependant claims 2-5 contain all of the limitations of claim 1. Accordingly, for at least the reasons discussed above with respect to claim 1, Applicants submit that the rejection of claims 2-5 should also be withdrawn.

Furthermore, in the Office Action, the same bases for rejection of claims 1-5 were applied to claims 17-20 and 33-36. Applicants submit that for at least the same reasons discussion above, i.e., because Fak fails to disclose one or more limitations of claims 17-20 and claims 33-36, the rejection of these claims in view of Fak should also be withdrawn.

With regard to the §102(b) rejections of claims 1, 6, 7, 12, 17, 22, 23, 28, 33, 38, 39, and 44 as anticipated by Konheim, amended independent claims 1, 17 and 33 each include limitations regarding, *inter alia*, performance of a cryptographic operation upon an ATM PIN in order to create a non-ATM PIN for use in a non-ATM electronic transaction. Konheim describes a cryptographic architecture for improving the security of cash-issuing or similar terminal systems when it is necessary to operate off-host. (See Konhaim, Abstract). As an initial matter, Konheim relates to various customer

identification operations that are performed by a controller. (See Konheim, Abstract). The operations performed according to Konheim are performed without any user input between operations. This forecloses the possibility of utilizing any numbers generated during the procedure in the context of a second electronic commerce transaction which is of a different type from the first, as is recited in the claims of the present invention.

Moreover, the portion of the Office Action which cites Fig. 5A of Konheim equates several variables of Konheim, i.e., "M1" and "M2," with the ATM PIN and non-ATM PIN of the present invention. (See Office Action, p. 5). However, M1 and M2 are defined as an account number and the output of some computation which is performed on an account number, respectively. (See Konheim, col. 13, lines 30-42). Accordingly, because Konheim fails to disclose at least these features of independent claims 1, 17 and 33 as amended, Applicants respectfully request that this rejection be withdrawn. Additionally, because dependent claims 6, 12, 22, 23, 28, 33, 38, 39, and 44 inherently contain the limitations of independent claims 1, 17 and 33, at least for the reasons discussed above, Applicants respectfully request that the rejection be withdrawn as to these claims as well.

With regard to the §102(b) rejections of claims 14, 15, 30, 31, 46 and 47 as anticipated by Rosenow, independent claims 14, 30, and 46 were modified in a prior Amendment, dated Oct. 22, 2003, to recite a technique for "generating a cryptography key which corresponds to a bank or issuer identification number." Applicants respectfully request consideration of this Amendment and Applicants' supporting Remarks filed concurrently therewith, which Applicants do not believe the Examiner addressed previously.

Rosenow describes a fault-tolerant arrangement for use in a multichannel data encryption unit. (See Rosenow, Abstract). The portion of Rosenow which is cited in the Office Action at p. 6 describes methods for generating customer PINs using cryptographic operations. (See Rosenow, col. 18, lines 26-40). However, Rosenow fails to disclose generating a cryptography key which corresponds to a bank or issuer identification number. In fact, the Examiner does not even assert that Rosenow discloses this limitation. Accordingly, Applicants respectfully request that that this objection be withdrawn.

Regarding the §102(b) rejections of claims 49 and 50 as anticipated by Rosenow, independent claim 49 has been amended to include the following limitations, *inter alia*:

> performing a cryptographic operation upon the first set of identification data to generate a second set of identification data for use in conducting said non-ATM electronic financial transaction, wherein said first set of identification data is an ATM PIN, said first transaction type is an ATM-transaction, said second set of identification data is a non-ATM electronic commerce PIN, and
>
> performing a second cryptographic operation upon said non-ATM electronic commerce PIN to generate said ATM PIN.

The cited portions of Rosenow describe the encryption of a PIN number during an ATM transaction, and transmission of the encrypted PIN to facilitate completion of the ATM transaction. (Rosenow, col. 17, lines 1-6). Rosenow does not, however, teach performing a cryptographic operation on an ATM PIN to generate a second PIN number for use in other electronic transactions which are not ATM transactions, as these limitations are recited in amended claim 49. It is therefore respectfully requested that this rejection of amended independent claim 49 and corresponding dependent claim 50 be withdrawn.

Claim rejections under 35 U.S.C. § 103(a)

Claims 8-11, 13, 24-29, 40-43, and 45 were rejected under 35 U.S.C. §103(a) as being unpatentable over Konheim; claims 16, 32, and 48 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rosenow in view of Ford et al., "Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption" (hereinafter "Ford"); claims 21 and 37 were rejected under 35 U.S.C. §103(a) as being unpatentable over Fak in view of Ford. Reconsideration of the rejections of record is respectfully requested.

With regard to the §103(a) rejections of claims 8-11, 13, 24-29, 40-43 and 45, these claims include all the limitations of the claims on which they depend, namely claims 1, 17 and 39. Each of these independent claims recite performing a cryptographic operation on an ATM PIN to generate a non-ATM PIN for use in another electronic transaction which is a non-ATM transaction. As discussed above, this feature is not taught or suggested in Konheim or any other reference cited in the Office Action. Accordingly, because Konheim fails to teach or suggest at least this limitation of claims 8-11, 13, 24-29, 40-43 and 45, Applicants respectfully request that this rejection be withdrawn.

With regard to the §103(a) rejections of claims 16, 32, and 48 as unpatentable over Rosenow in view of Ford, these dependent claims include all the limitations of the claims on which they depend, including amended independent claims 14, 30, and 46 which require the generation of a cryptography key which is specific to each bank or issuer and which is generated by using a key derivation key in a cryptographic operation performed on data obtained from an identification number. This technique is not taught

or even remotely suggested by Rosenow, either viewed alone or in concert with Ford. Accordingly, Applicants respectfully submit that claims 16, 32, and 48 are in condition for allowance.

Claims 21 and 37 were also rejected under §103(a) as unpatentable over Fak in view of Ford. These claims depend on independent claims 17 and 33, respectively, which include the limitation, *inter alia*, of performing a cryptographic operation upon an ATM PIN to generate a second PIN related to a non-ATM electronic transaction. Fak and Ford taken alone or in combination fail to teach or suggest at least this limitation contained in claims 21 and 37 by virtue of their dependency from claims 12 and 33. Accordingly, Applicants respectfully submit that claims 21 and 37 are in condition for allowance.

CONCLUSION

In view of the foregoing, Applicants submit that claims 1-50 as amended, all of the pending claims, are in condition for allowance. In the event that the application is not deemed in condition for allowance, the Examiner is invited to contact the undersigned in an effort to advance the prosecution of this application.

Respectfully submitted,

Robert C. Scheinfeld
Patent Office Reg. No. 31,300

BAKER BOTTS, L.L.P.
30 Rockefeller Plaza
New York, New York 10112-4498

Attorneys for Applicants
(212) 408-2512

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Please replace the section entitled "BRIEF DESCRIPTION OF THE DRAWINGS" on pages 4-5 of the Specification with the following:

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in greater detail below by reference to the drawings, in which:

FIG. 1 is a flow chart of an exemplary procedure for generating a conversion key in accordance with the invention;

FIG. 2 is a flow chart of an exemplary procedure for generating a key-check value in accordance with the invention;

FIG. 3 is a flow chart of an exemplary procedure for generating an Electronic-Commerce PIN from the ATM PIN in accordance with the invention; and

FIG. 4 is a flow chart of an exemplary procedure for converting an Electronic-Commerce PIN into an ATM PIN in accordance with the invention; and

FIG. 5 is a diagram of an exemplary system accordance with the invention.

IN THE CLAIMS:

Please amend the claims as follows:

1. (Amended) A method for generating identification data, comprising the steps of:

providing [a first set of identification data] an ATM PIN related to a first transaction type which is an ATM transaction; and

performing a cryptographic operation upon the [first set of identification data] ATM PIN, thereby generating a [second set of identification data related to a second transaction type] non-ATM electronic commerce PIN for use in a second transaction which is a non-ATM transaction.

2. (Amended) A method according to claim 1, wherein the step of performing a cryptographic operation comprises:

providing a conversion key; and

using the conversion key to perform said cryptographic operation upon the [first set of identification data] ATM PIN.

6. (Amended) A method according to claim 1, wherein the step of performing a cryptographic operation comprises:

providing cryptographically-computed data; and

performing an operation upon the [first set of identification data] ATM PIN and the cryptographically-computed data.

10. (Amended) A method according to claim 9, wherein the operation upon the [first set of identification data] ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

11. (Amended) A method according to claim 10, wherein the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the [first set of identification data] ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the [first set of identification data] ATM PIN.

12. (Amended) A method according to claim 6, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the [first set of identification data] ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the [first set of identification data] ATM PIN.

13. (Amended) A method according to claim 6, wherein the operation upon the [first set of identification data] ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

17. (Amended) A system for generating identification data, comprising:

a memory for storing [a first set of identification data related to a first transaction type]an ATM PIN; and

a processor for performing a cryptographic operation upon the [first set of data] ATM PIN, such that said processor generates a second [set of identification data related to a second transaction type] non-ATM PIN related to a non-ATM electronic transaction.

18. (Amended) The system of claim 17, wherein the memory includes means for storing a conversion key, and wherein the processor comprises means for using the conversion key to perform a cryptographic operation upon the [first set of identification data] ATM PIN.

22. (Amended) The system of claim 17, wherein the memory includes means for storing cryptographically-computed data, and wherein the processor comprises:

means for generating the cryptographically-computed data; and

means for performing an operation upon the [first set of identification data] ATM PIN and the cryptographically-computed data.

26. (Amended) The system of claim 25, wherein the means for performing an operation upon the [first set of identification data] ATM PIN and the cryptographically-computed data comprises either a subtraction means or an addition means.

27. (Amended) The system of claim 25, wherein the means for performing an operation further comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing the [first set of

identification data] ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the [first set of identification data] ATM PIN.

28. (Amended) The system of claim 22, wherein the means for performing an operation comprises means for generating a cryptographically-computed number having a base corresponding to a base of a number representing [first set of identification data] ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the [first set of identification data] ATM PIN.

33. (Amended) A system for generating identification data, comprising:

a memory;

a processor in communication with the memory; and

a computer-readable medium in communication with the processor and storing instructions which, when executed, cause the processor to perform the steps of:

storing [a first set of identification data] an ATM PIN in the memory, said first set being related to a first transaction type; and

performing a cryptographic operation upon the [first set of identification data] ATM PIN, thereby generating a second [set of identification data related to a second transaction type] PIN related to a non-ATM electronic transaction..

34. (Amended) The system of claim 33, wherein the step of performing a cryptographic operation comprises:

providing a conversion key;

storing the conversion key in the memory; and

using the conversion key to perform said cryptographic operation upon the [first set of identification data] ATM PIN.

38. (Amended) The system of claim 33, wherein the step of performing a cryptographic operation comprises:

providing cryptographically-computed data;

storing the cryptographically-computed data in the memory; and

performing an operation upon the [first set of identification data] ATM PIN and the cryptographically-computed data.

41. (Amended) [A method according to claim 40] The system of claim 40, wherein at least a portion of the initial data is obtained from at least a portion of an account number.

42. (Amended) The system of claim 41, wherein the operation upon the [first set of identification data] ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

43. (Amended) The system of claim 42, wherein the step of providing cryptographically-computed data further comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the [first set of identification data] ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing the [first set of identification data] ATM PIN.

44. (Amended) The system of claim 38, wherein the step of providing cryptographically-computed data comprises generating a cryptographically-computed number having a base corresponding to a base of a number representing the [first set of identification data] ATM PIN, wherein said cryptographically-computed number has a number of digits corresponding to a number of digits of said number representing [first set of identification data] ATM PIN.

45. (Amended) The system of claim 38, wherein the operation upon the [first set of identification data] ATM PIN and the cryptographically-computed data comprises either a subtraction operation or an addition operation.

49. (Twice Amended) A method for generating identification data for [an] a non-ATM electronic financial transaction over a communications network, comprising the steps of:

providing a first set of identification data related to a first transaction type;

performing a cryptographic operation upon the first set of identification data to generate a second set of identification data for use in conducting said non-ATM electronic financial transaction, wherein said first set of identification data is an ATM PIN, said first transaction type is an ATM-transaction, said second set of identification data is a non-ATM electronic commerce PIN[which is of a different type from said first transaction.]; and

performing a second cryptographic operation upon said non-ATM electronic commerce PIN to generate said ATM PIN.

50. (Amended) The method of claim 49, [wherein said first set of identification data is an ATM-PIN, said first transaction type is an ATM-transaction, said second set of identification data is an electronic commerce PIN, said electronic financial transaction is an electronic commerce transaction, said method] further comprising the step of:

performing a second cryptographic operation upon said electronic commerce PIN to generate said ATM-PIN.

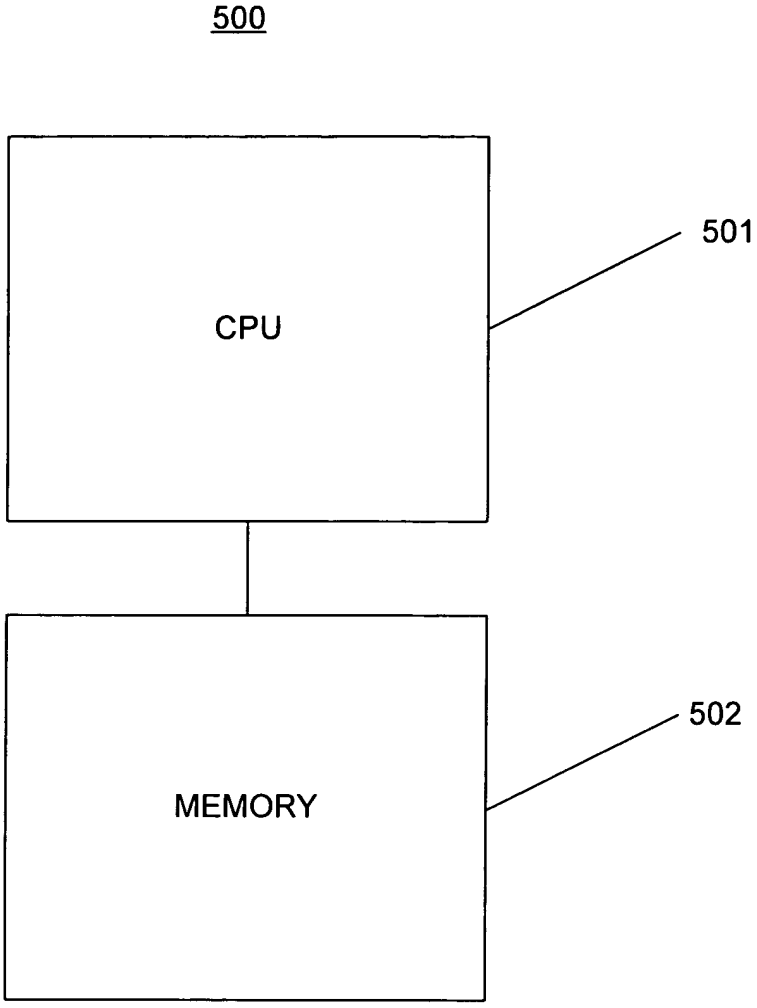

FIG. 5